

Building resilient digital workspaces for the public sector

Today's government agencies find it challenging to efficiently deliver virtual desktops and apps, manage a growing number of endpoints, and gain visibility into IT operations. Omnissa addresses these challenges with a unified IT management platform providing centralized visibility and modern solutions for secure **virtual apps and desktops**, **digital employee experience**, robust **security and compliance**, and **unified endpoint management**. This **comprehensive platform** enables government agencies to protect data, ensure compliance, and streamline operations with a real-time, unified view across systems and endpoints for greater operational agility.



At a glance

Enhance visibility, security, and efficiency for your government agency with a unified platform offering endpoint management, virtual desktops and apps, and compliance tools.

Some examples of what Omnissa can help you do

- Provide secure virtual desktops and remote access to government employees.
- Manage diverse endpoint fleets with centralized security policies.
- Automate compliance audits and vulnerability management.
- Enable continuous monitoring and threat detection across departments.
- Support hybrid work models with secure device management.

omnissa™



Omnissa streamlines IT management into a single platform, reducing complexity and costs while enhancing security and efficiency. By automating tasks and integrating analytics, it eases the burden on your IT teams and improves productivity. With flexible, scalable deployments and open ecosystem support across hybrid cloud and on-premises environments, Omnissa can help your agency protect data, optimize workflows, and adapt to evolving digital demands with ease.

Omnissa platform features and benefits

Feature	Description	Benefits for government
Centralized device management	Unified control and monitoring of all devices and endpoints across your agency	Simplifies IT operations, reduces manual effort, and improves consistency and control
Zero trust security and threat detection	Continuous security monitoring and strict access policies based on device and users	Enhances data protection, reduces risk of breaches, and supports compliance
Intelligent automation and workflow	Automate routine IT tasks like patching, compliance checks, and incident response	Improves operational efficiency, reduces IT workload, speeds response times, and reduces human error
Unified endpoint management (UEM)	Manage apps, patches, and policies on all devices including mobile and legacy endpoints	Streamlines management of hybrid and mobile work environments, and supports consistent security and compliance enforcement
Secure virtual desktop infrastructure (VDI)	Deliver and manage virtual desktops and apps in the cloud or on-premises	Supports flexible access for remote work, extends hardware lifecycles, and helps ensure business continuity
Data-driven insights and analytics	Real-time visibility into system health with machine learning for proactive management	Enables proactive issue resolution, and informs policy and resource allocation with actionable KPIs that anticipate and mitigate risks
Flexible work environment support	Support hybrid work models with secure access from any device or location through agency-owned and BYOD devices	Enhances workforce productivity and reduces friction
Automated compliance and reporting	Tools to help automate audits to meet regulatory standards (NIST, HIPAA, CJIS) with audit-ready logs	Simplifies adherence to government frameworks and complex regulations

Get started

Empower your agency with unmatched IT visibility, security, and resilience through advanced endpoint management, secure virtual desktops, and real-time insights. Visit our [public sector webpage](#) to take the first step.